

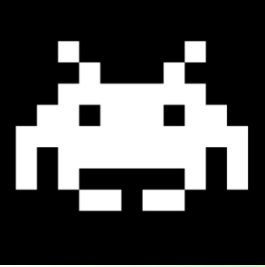
INSERT COIN

BOTNETS

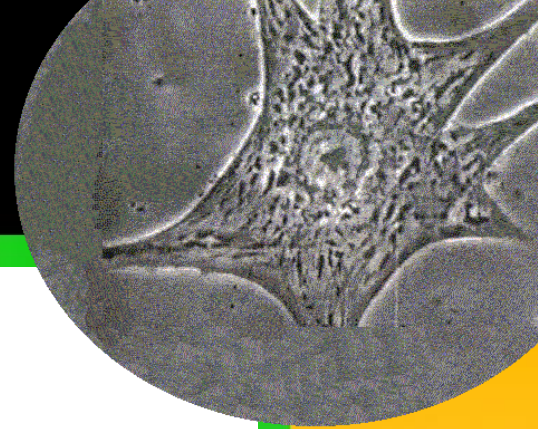


Taller de
Informatica
Focense

matias porolli
UTN
2011

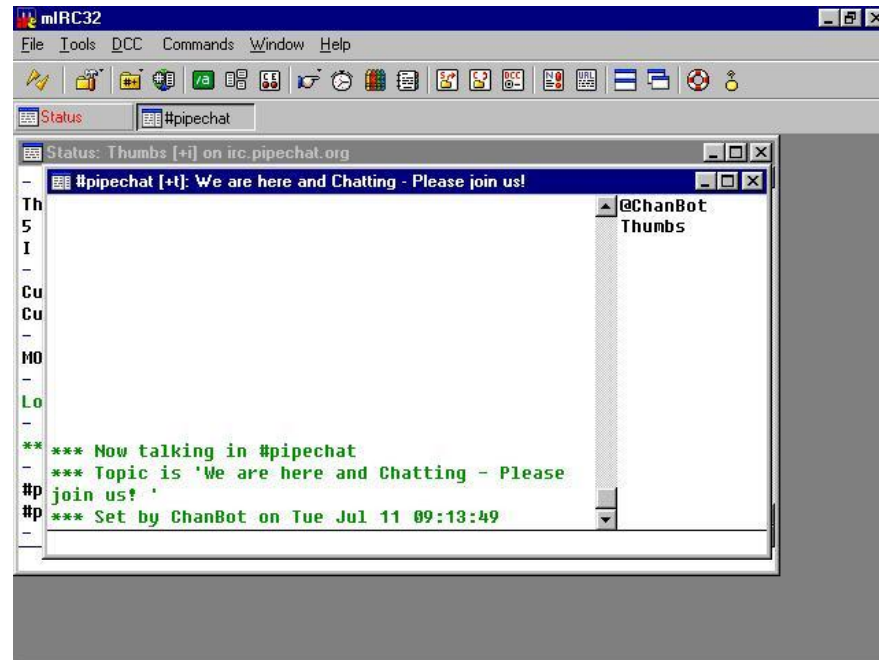


Historia



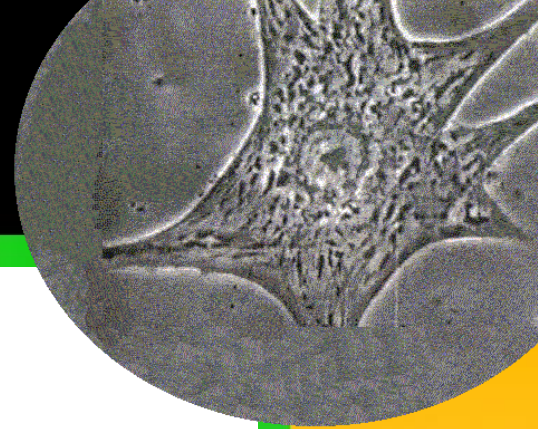
1988 IRC

- Chat grupal / individual
- Cliente – Servidor
- Administradores





Historia



1989GM

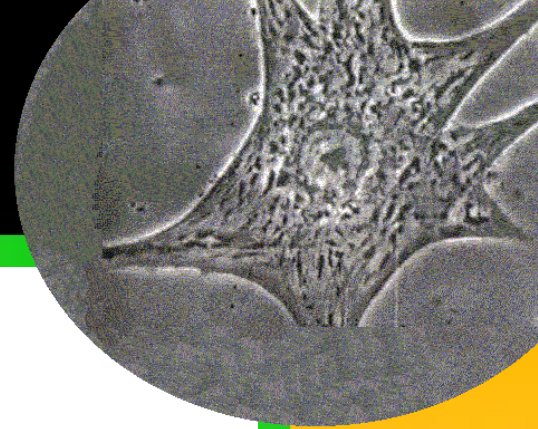
- Uno de los primeros bots
- Bot: script que se comporta como usuario
- Juega “Caza al Wumpus” contra humanos

- Remplazar al administrador
- Realizar tareas rutinarias





Historia



1999 Pretty Park

- Código Malicioso: gusano
- Obtiene info del sistema
- Realiza harvesting
- Descarga de archivos

1999 SubSeven

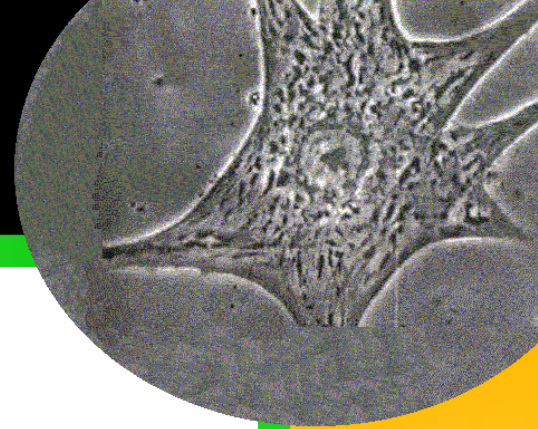
- Código Malicioso: troyano
- Permite control del sistema



pirate



Historia

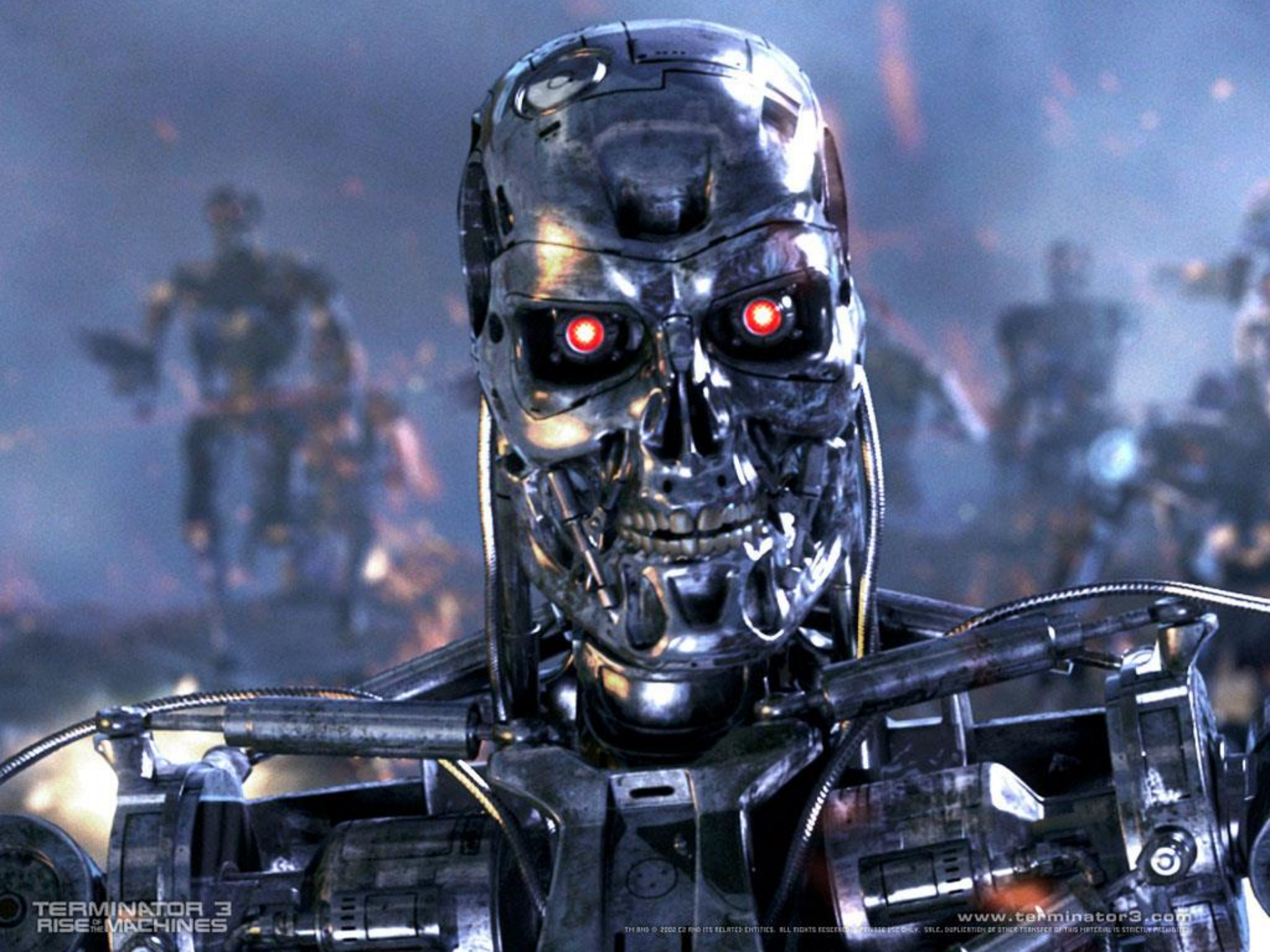


— — Ideas básicas

- Medio de Comunicación y Control
- Bot escucha canal IRC, espera comandos
- Control remoto, automatización
- Descarga de archivos

— — Código malicioso

- Antes: diversión, conocimiento, reto
- Ahora: \$\$\$, crimen, mafia



TERMINATOR 3
RISE OF THE MACHINES

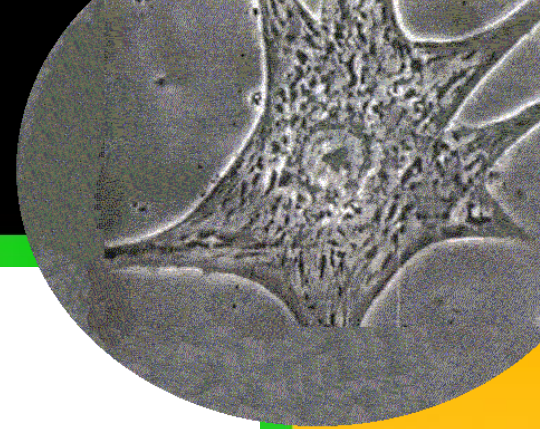
www.terminator3.com

TM, ® & © 2003 C2 AND ITS RELATED ENTITIES. ALL RIGHTS RESERVED. NO TRADE USE ONLY. SELC. DUPLICATION OR OTHER TRANSFER OF THIS MATERIAL IS STRICTLY PROHIBITED.





Historia



2000GT Bot

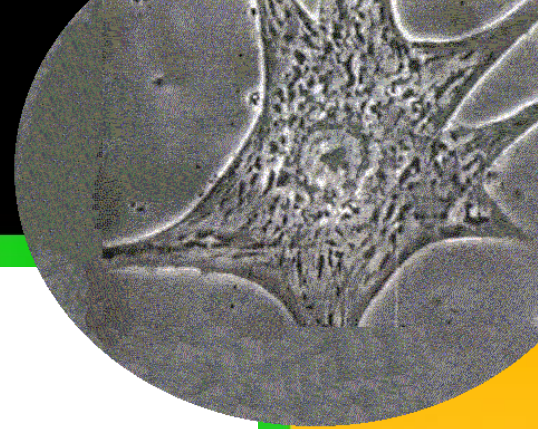
- Basado en mIRC
- Oculta su presencia en el sistema
- Ejecución remota de procesos
- Acceso anónimo al servidor IRC

2002SDBot

- De código abierto
- Muy simple
- Da lugar a cientos de bots similares con distintas funciones



Historia



2002 Agobot

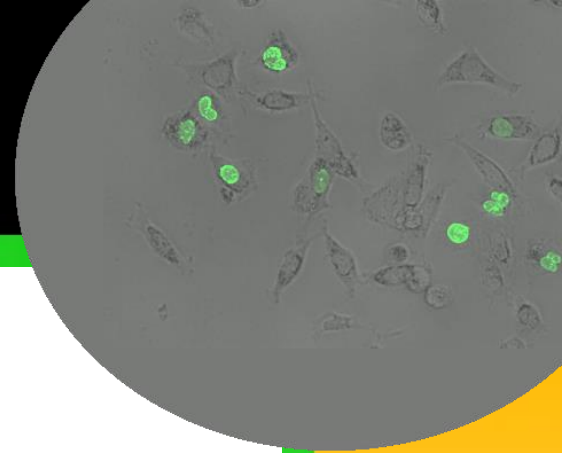
- Diseño modular
- Los módulos se obtienen por etapas

Por ejemplo:

- Módulo 1: cliente IRC, backdoor
- Módulo 2: mata procesos antivirus
- Módulo 3: bloquea acceso sitios web
- Módulo n: payload



Conceptos



>Bots

- Programas que automatizan tareas

>Zombies

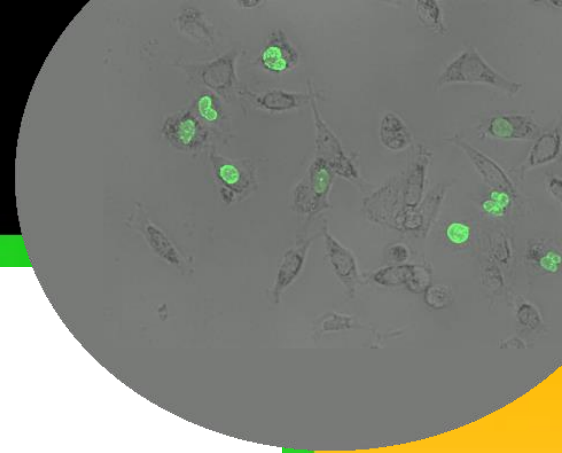
- Computadoras infectadas por el bot

>Botnets

- Redes de zombies controlados en forma remota
- Sin consentimiento o conocimiento

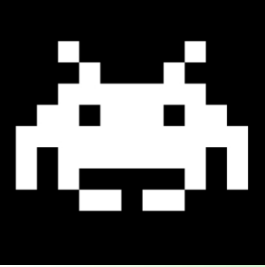


Conceptos



Botnets Una definición

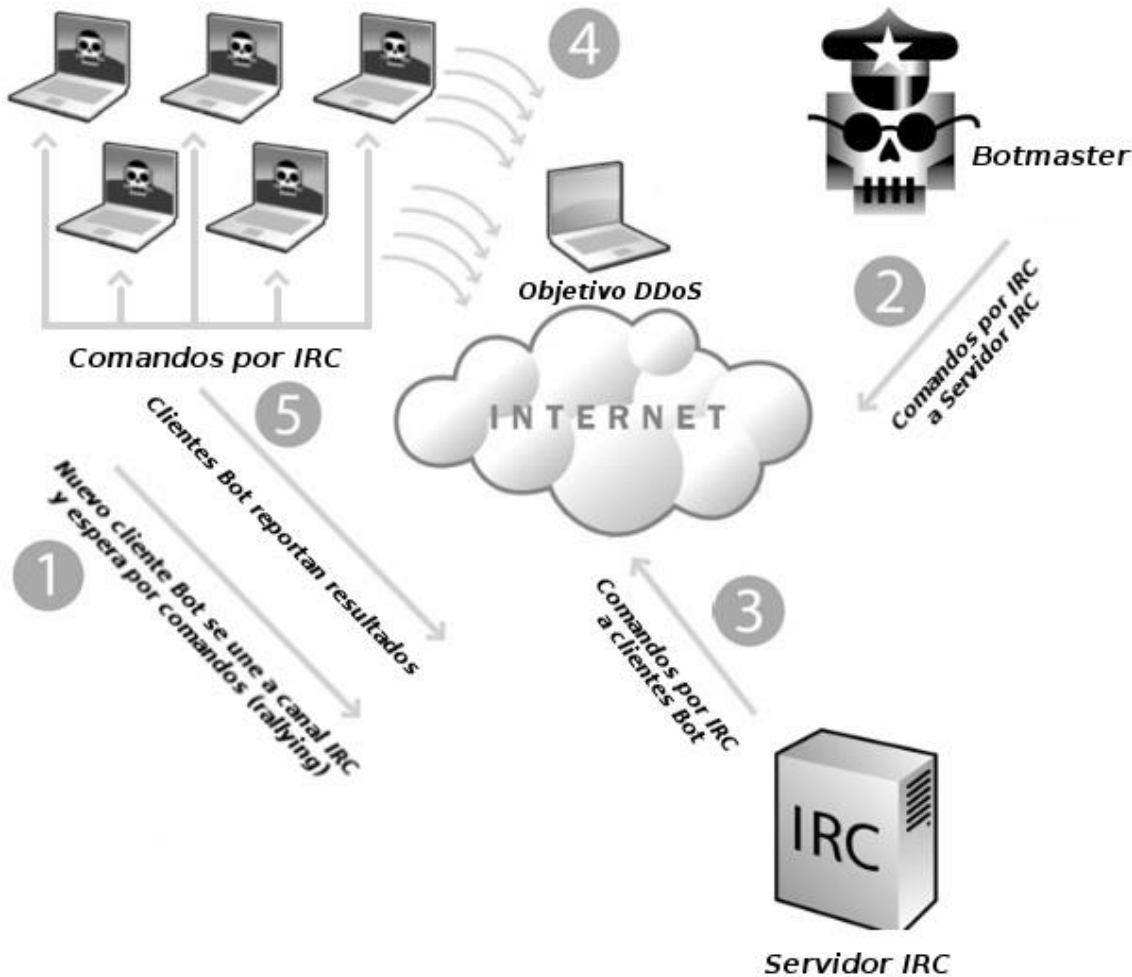
“una red de sistemas interconectados, bajo el control expreso de una entidad remota, cada uno de los cuales es vulnerado por uno o más bots, y usado para realizar tareas y ataques que pueden ser llevados a cabo de forma más efectiva por muchas máquinas conectadas que por las máquinas aisladas”

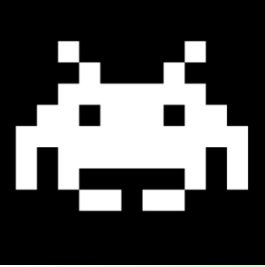


Command&Control



C&C por IRC

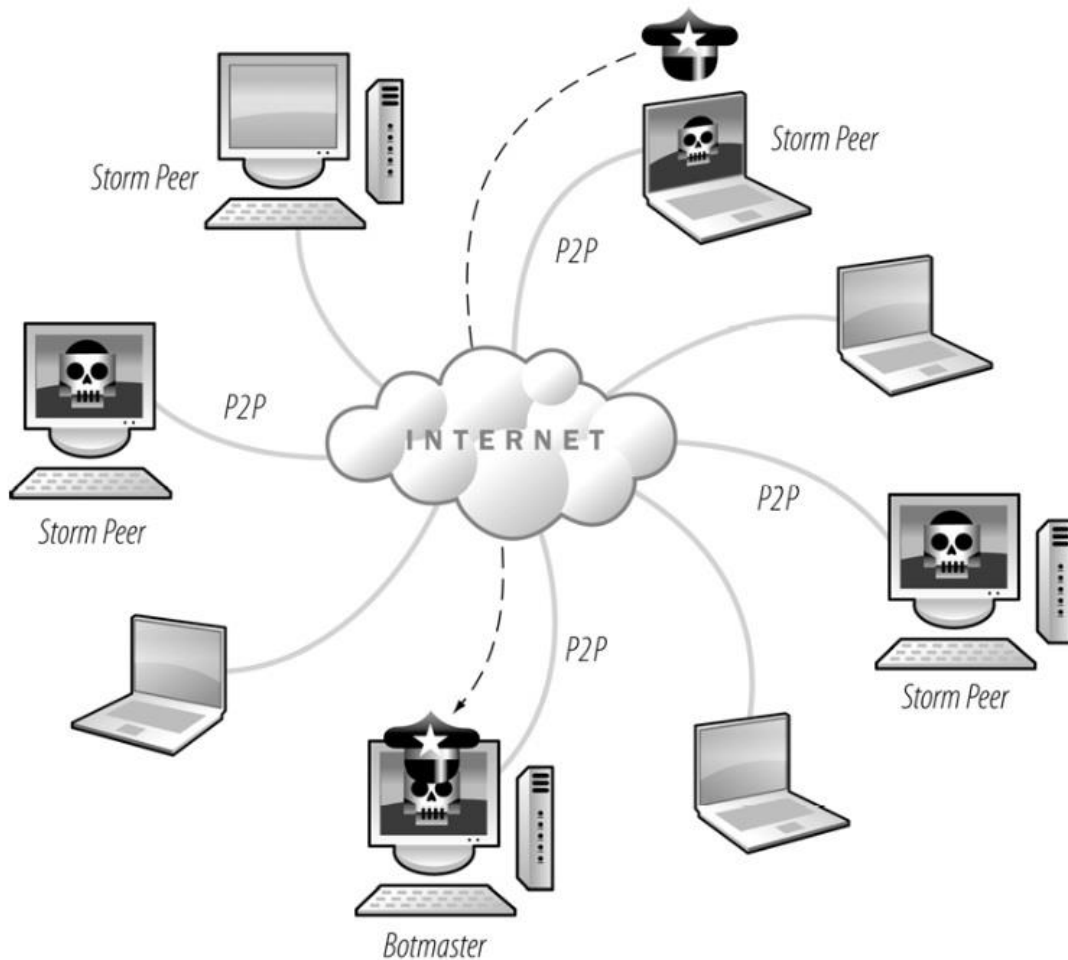




Command&Control



C&C por P2P



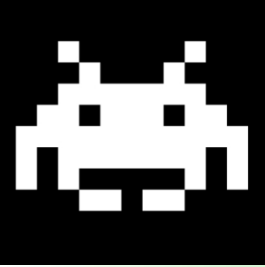


C&C por P2P

- Peers
- Botmaster determina servidores
- Módulos distribuidos. Listas de archivos
- Distribución de comandos: pull / push

C&C por HTTP

- Modelo centralizado (similar IRC)
- Comunicación bajo demanda
- Se mezcla con tráfico de Internet
- Kits listos, fáciles de usar



Command&Control



C&C por HTTP

[statistics][control] [help] Zünker Panel v1.4.5b [LOG OUT]

[Global] [Downloaded files][Time statistics]

Bot traffic Statistics for www [REDACTED] generated on 2007/04/25

Zupacha Mini stats

Protocol	Sent Msg
Spam-bots mail	1493082 80%
Mirabilis ICQ	184027 10%
E-Mail	181619 10%
Web mail	10067 1%
Aol AIM	809 0%
Web forum	201 0%
Yahoo! IM	189 0%
Google Talk	3 0%

Totally Sent : 1,869,997

Service name	Sent Msg
mail.yahoo.com	5072 50%
mail.google.com/mail/	3240 32%
hotmail.msn.com	966 10%
webmail.aol.com	616 6%
Mail.ru	117 1%
rambler.ru	56 1%
comcast.net	0 0%
mail.com	0 0%
lycos.com	0 0%
earthlink.net	0 0%
care2.com	0 0%

Web mail Sent : 10067

phpBB

Topic reply:

New topic messages:

VBulletin

Topic reply:

New topic messages:

Forum messages totally: 201

Country	Rating
Germany	10602 95%
Russia	179 2%
United States	81 1%
Austria	60 1%
France	26 0%
Switzerland	24 0%
Poland	19 0%
Spain	19 0%
United Kingdom	17 0%
Hungary	15 0%
Netherlands	10 0%
Czech Republic	9 0%
Belgium	7 0%
Mexico	6 0%
Brazil	5 0%
Iraq	5 0%
Italy	5 0%
Slovakia	5 0%
Turkey	5 0%
Greece	5 0%

Totally: 52

Country	Rating
Germany	25 93%
Czech Republic	1 4%
Russia	1 4%

totally: 27

Country	Rating
Germany	779693 93%
Russia	16807 2%
United States	11196 1%
Austria	5025 1%
France	3452 0%
Spain	3226 0%
Poland	1943 0%
Switzerland	1693 0%
Hungary	1474 0%
United Kingdom	1411 0%

Totally bot's reports: 838750

Top 10 bot versions

Bot version	Rating
3.2.7	11160 100%

Totally: 1

Top Anti-virus-spyware software. Select Country: [Go to Detailed](#)

Software	Rating	Country	Rating
Anti Virus	0	Anti Virus	
Soft names	Totally: 0		
Software installed:	0		

Sumarize

Bot's count: 11160 Today new bots: 350 Today Bot reports: 5596
All New bot today: 27 Percent Live bot's: 50% Bot reports: 838750 Oldest bot has: 19 days



DNS Dinámico_Fast Flux

- Asignar pool de IPs a un dominio
- Rotar rápidamente
- Utilizar varios nombres de dominio

Proxies

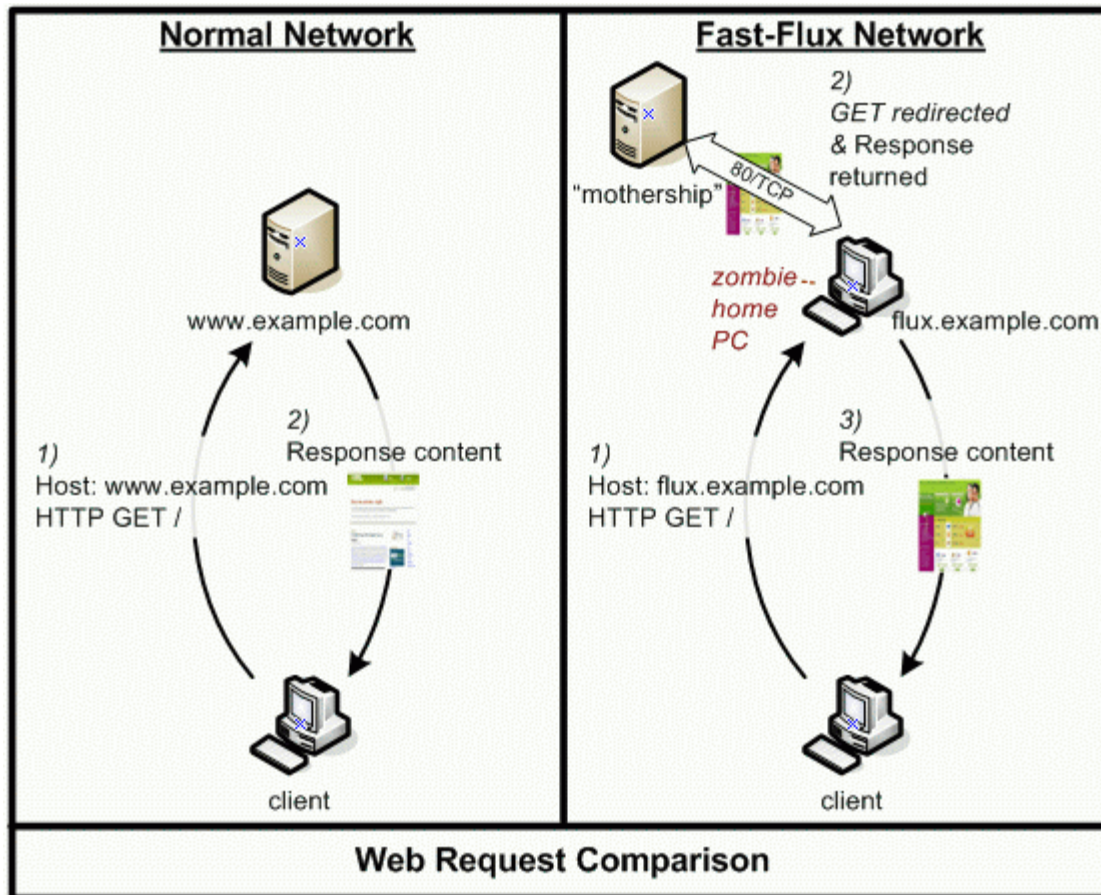
- Comunicación indirecta con los servidores
- Se pueden utilizar varios niveles
- Promoción / Degradación



Otras tecnicas

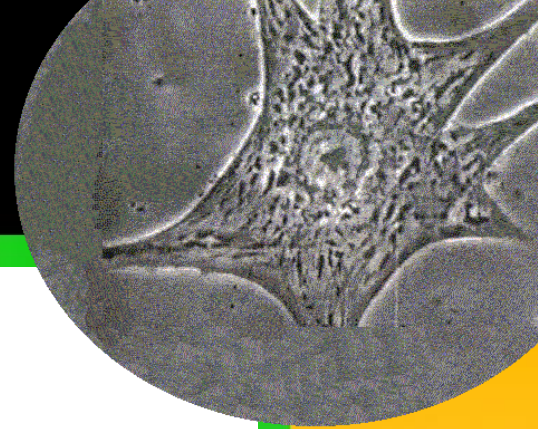


Ejemplo





Ataques



>Autopropagación

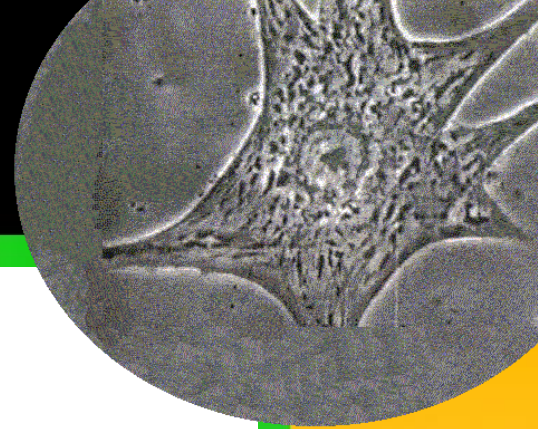
- Reclutar zombies

>Spam

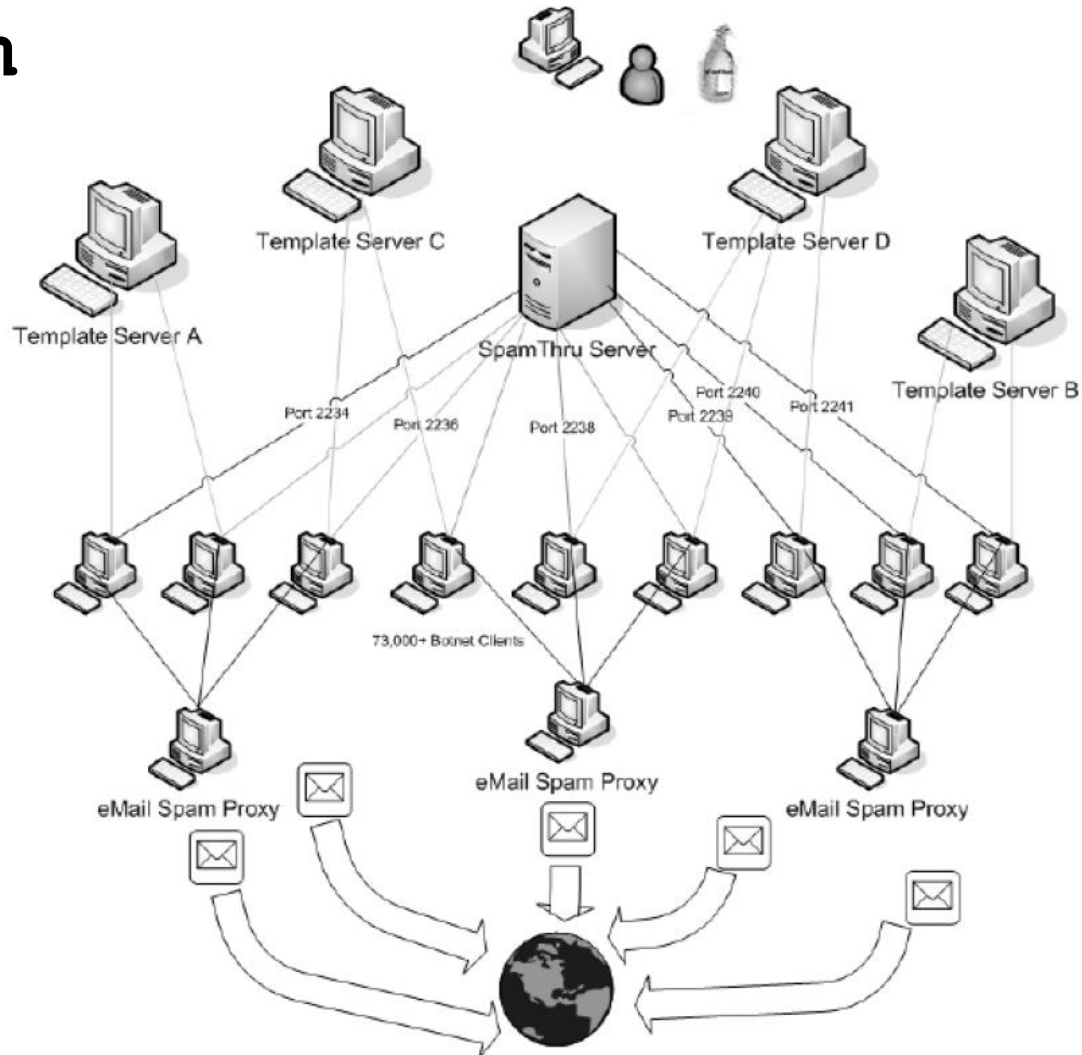
- Distintas plantillas a distintos grupos de zombies
- Proxies
- 1 respuesta cada 12.5 millones de e-mails
- 80% de e-mails son spam, 80% de botnets



Ataques

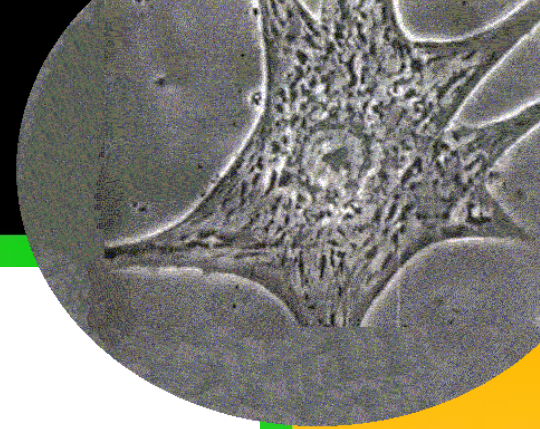


> Spam





Ataques

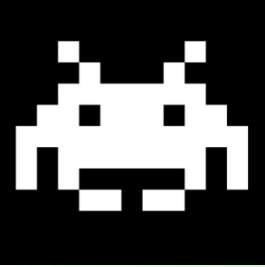


>DDoS

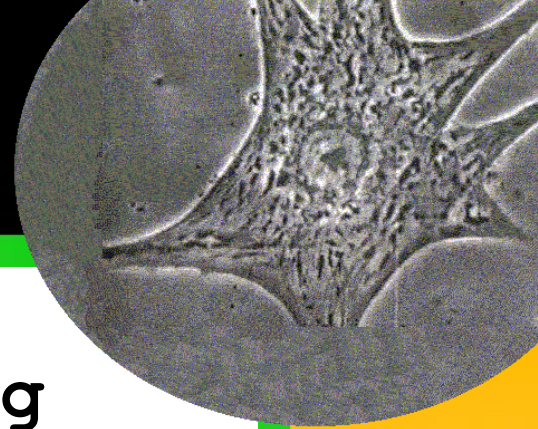
- Inundación
- Paquetes SYN. Conexión
- Extorsión. Alquiler

>Adware y Fraude por clicks

- Google AdSense
- 15% de los clicks son fraudulentos
- Pago por instalación de adware

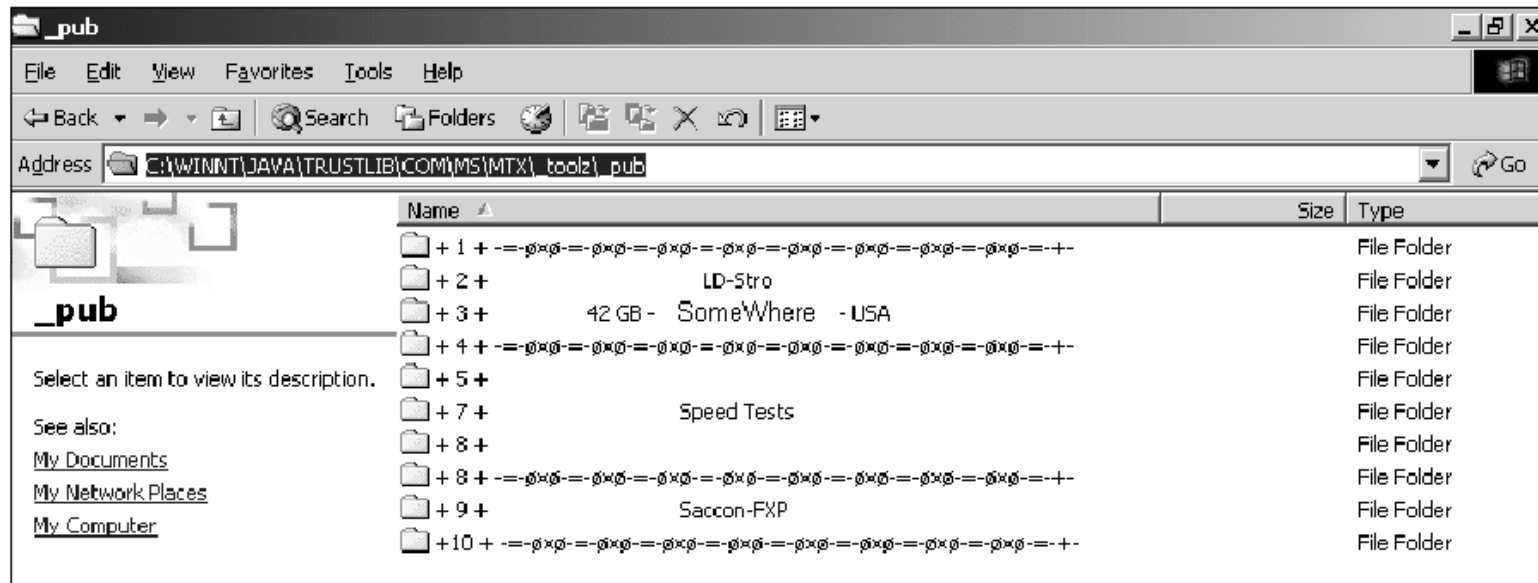


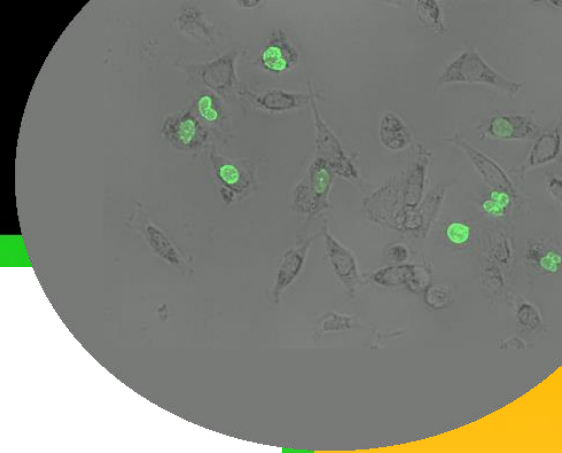
Ataques



>Phishing, pharming, keylogging

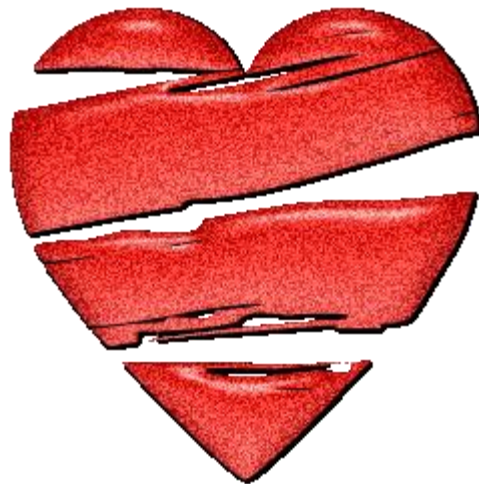
>Almacenamiento de información ilegal

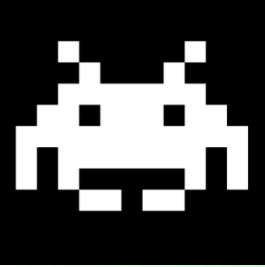




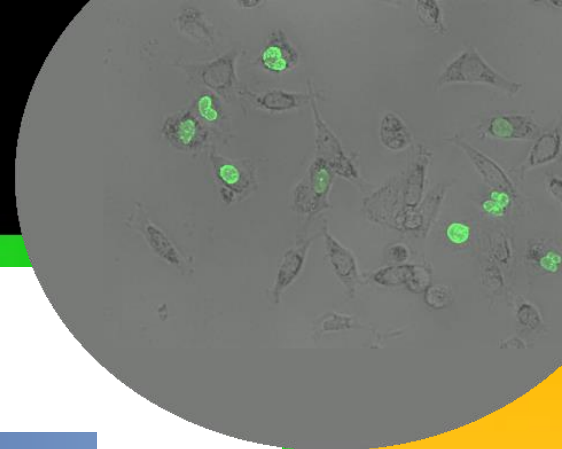
2009Waledac

- Troyano
- Esparcimiento masivo en San Valentín (2009)
- Distribuido mediante spam
- Utilizado para generar spam
- 100 000 zombies





Intervenciones



Caroline has sent you a Valentine's Day E-Card! - Mensaje (HTML)

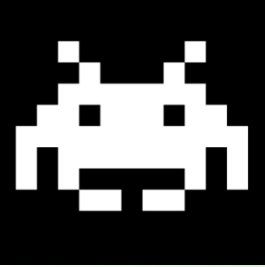
Archivo Edición Ver Insertar Formato Herramientas Acciones ?

Responder Responder a todos Reenviar [Icons]

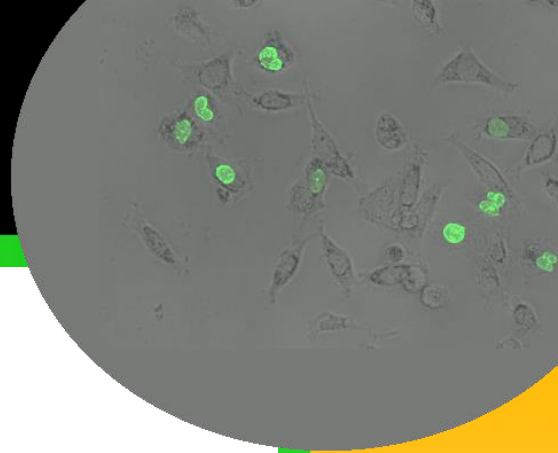
De: Caroline Enviado el: Viernes 06/02/2009 11:55 a.m.
Para:
CC:
Asunto: Caroline has sent you a Valentine's Day E-Card!

Caroline just sent a greeting e-card and wrote to you:
"Yeah I Love You"

Click on the link below to view your Valentine's Day card:
<http://www.██████████.online.com/?carid=235>





Intervenciones

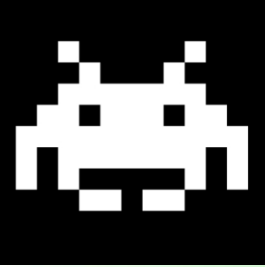


http://t[redacted].com/

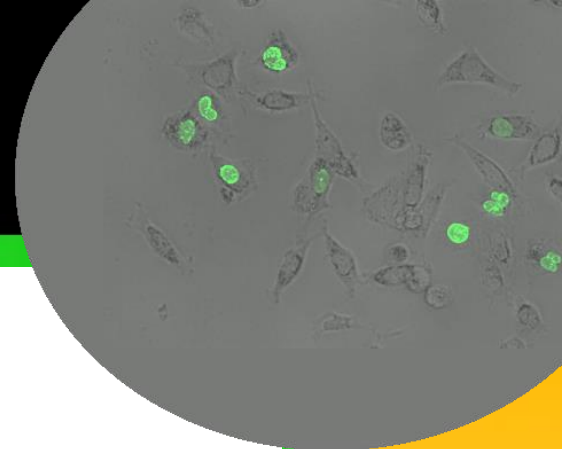
Guess, which one is for you?

http://t[redacted].com/you.exe



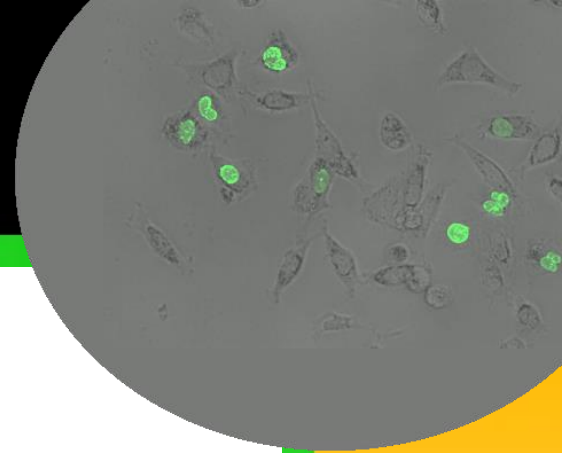
Intervenciones



>Waledac

Luego de que Microsoft presentara una denuncia ante la corte estadounidense de Virginia, el 22 de febrero de 2010 el juzgado federal forzó el cierre de 277 dominios de Internet utilizados por la botnet





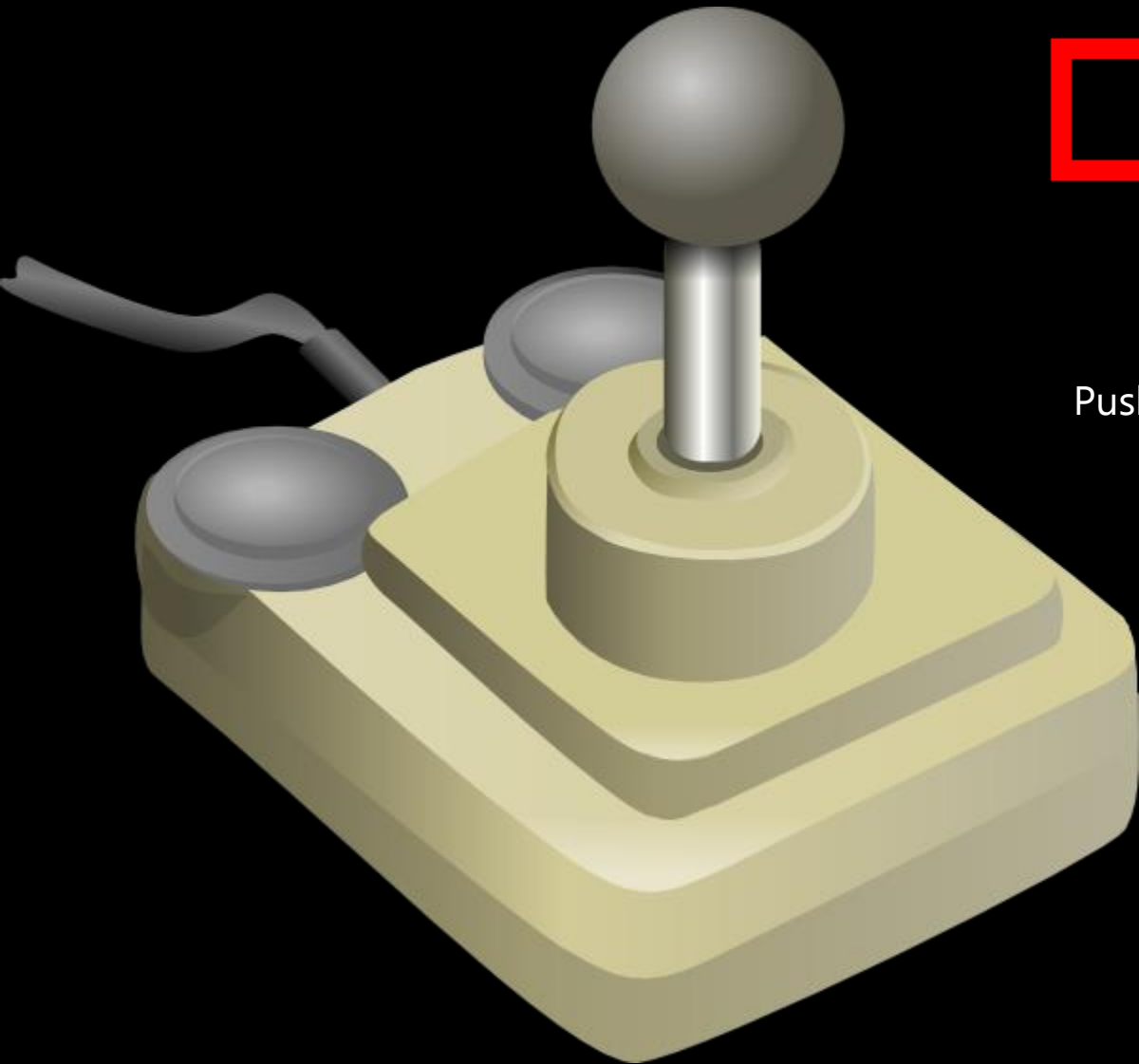
2010 Bredolab

- Difundía spam y era alquilada
- 30 millones de zombies
- Desmantelada por el gobierno holandés y profesionales de seguridad

2011 Rustock

2011 Coreflood

⋮



DEMO

Push any Button



*Grazie
Bambini!!*